



Gen Reveals Cybersecurity Predictions for 2025

2024-12-04

AI will begin to blur reality, data theft will pave the way for identity theft, and scams will become hyper-personalized and data-driven following a year of large-scale breaches

TEMPE, Ariz. and PRAGUE, Dec. 4, 2024 /PRNewswire/ -- [Gen](#)™ (NASDAQ: GEN), a global leader dedicated to powering Digital Freedom through its family of Cyber Safety brands, today released its top cyberthreat predictions for 2025. Gen cybersecurity experts predict the next phase of AI and deepfakes, a shift in data theft towards full-scale identity theft, ultra-sophisticated scams and new tactics for financial theft.

"After a monumental year in AI – and a somewhat catastrophic year in breaches – we believe we'll see significant shifts in both scams and digital identity risks in 2025," said Siggi Stefnisson, Cyber Safety CTO at Gen. "Cybercriminals will capitalize on large breaches to either steal identities outright or utilize the information to create hyper-personalized and believable scams. AI will exasperate the issues, not only helping criminals make their scams more sophisticated, but also forcing people to question how the technology is shaping human thought. It's sure to be a year of change, and it will be more important than ever for people to be protective of their digital lives."

Gen's Top Cyber Predictions for 2025:

AI will start to blur everyday reality. Large Language Models (LLMs) will begin to create hyper-personalized experiences as people work more with AI. In late 2024, over 200 million people used ChatGPT on a weekly basis. While convenient, these technologies will likely begin shaping individual perceptions and reality, prompting ethical discussions on AI's impact on human thought. As AI becomes more integrated into complex areas like parenting and education, ethical concerns about its role in society will grow. We can anticipate more debate addressing the technology's boundaries and influence on personal development. The European Union and several US states have already introduced legislation to advance AI protections, and we expect that there will be increased activity across the US and around the world in the coming year.

Deepfakes will become unrecognizable. AI will become sophisticated enough that even experts may not be able to tell what's authentic. People will have to ask themselves every time they see an image or watch a video: is this real? Unfortunately, people with bad intentions will take advantage. This can be as personal as a scorned ex-partner spreading rumors via fake photos on social media or as extreme as governments manipulating entire populations by releasing videos that spread political misinformation. As deception becomes increasingly sophisticated, verifiable digital credentials – a combination of verifiable information used together as a digital authenticity signature – will evolve into powerful tools for proving what's real. As our realities become increasingly blurred by AI, this is an example of how to help ensure AI is used as a force for good, providing a critical foundation for maintaining trust online.

Data Theft leads to surge in Identity Theft. Following a year of consistent, large-scale breaches, we will continue to see a significant rise in identity theft. Criminals will stitch together personal information extracted from data breaches, publicly available sources, and information stolen from devices to create comprehensive profiles of individuals, putting individuals at higher risk of identity theft. This will fuel

sophisticated extortion attempts and enable attackers to convincingly impersonate trusted companies, especially those previously compromised.

Scams enter the era of hyper-personalization. We expect a shift towards hyper-personalized, human-centric methods that manipulate human behavior rather than exploiting traditional technological vulnerabilities. Armed with personal data from past breaches and dark web exchanges, attackers will develop hyper-targeted strategies to deceive their victims, similar to the [sextortion campaign we uncovered](#) in the US and Canada in 2024 which used Google Street View images to startle victims. Combining psychological insights and social engineering, these schemes will disarm people, deploying convincing phishing and fraud tactics across platforms like social media and messaging apps. Hyper-personalized, human-targeted methods will make it incredibly difficult to distinguish between legitimate communications and scams.

Financial Theft takes on new forms. We anticipate a notable surge in financial theft, driven by increasingly sophisticated mobile banking threats and the growing popularity of cryptocurrencies. Fraudsters will employ advanced techniques like deepfaked celebrities promising high ROI on their fake investment platforms, universal income announced by voice-cloned government officials or fake giveaways to deceive investors and traders alike. The [CryptoCore campaign](#) in 2024 showed signs of this future trend, taking over a million dollars from victims in just a few days leveraging Elon Musk deepfakes as a lure. Additionally, cybercrime and the physical world will collide as there are more cases of street muggers forcing people to unlock their phones and provide access to financial apps to transfer funds to attacker-controlled accounts.

How People Can Prepare:

- **Stay informed** – Scan the news and trusted security blogs to learn about the latest large-scale scams and data breaches.
- **Surf safely** – Using a Virtual Private Network (VPN) is one of the best ways to help protect your data and private information online.
- **Remain skeptical** – If it seems too good to be true, it usually is. Stop and think before you click on links or share information online.
- **Double-check** – Before you click on a link or share your personal or banking information, verify the source by searching their site directly. [Norton Genie](#) can also help you detect if a message is a scam.
- **Use trusted security tools** – Having all-in-one security like [Norton 360 Deluxe](#) or [Avast One](#) can help you protect your devices, personal information, and online privacy.
- **Be prepared in case you're impacted** – If your information ends up in the wrong hands, the best thing you can do is be alerted so you can take action. Tools like Dark Web Monitoring scan the dark web on your behalf and products like [LifeLock](#) can assist you if your identity is compromised.

To learn more about Gen's 2025 Predictions, keep an eye on [Gen LinkedIn](#) and read the [2025 Predictions Blog](#).

About Gen

[Gen](#)™ (NASDAQ: GEN) is a global company dedicated to powering Digital Freedom through its trusted Cyber Safety brands, Norton, Avast, LifeLock, Avira, AVG, ReputationDefender and CCleaner. The Gen family of consumer brands is rooted in providing safety for the first digital generations. Now, Gen empowers people to live their digital lives safely, privately, and confidently today and for generations to come. Gen brings award-winning products and services in cybersecurity, online privacy and identity protection to nearly 500 million users in more than 150 countries. Learn more at www.GenDigital.com.

View original content to download multimedia:<https://www.prnewswire.com/news-releases/gen-reveals-cybersecurity-predictions-for-2025-302322167.html>

SOURCE Gen Digital Inc.